

III. REMARKS

1. Claims 16, 18, 20, 24, 35 and 44 are amended, and claims 12, 17, 19, 21—25 and 43 are cancelled. Claims 45-48 are new.

2. Claims 2-4, 16-25 and 33-45 are not unpatentable over Kaydyk in view of either Ginter or Watanabe under 35 USC §103(a). The claims are amended to recite that the properties of a wireless communication device are examined, and a device-specific content component is selected from a set of different versions of device-specific content components to be loaded in a device specific content packet to the wireless communication device. At least these features are not disclosed or suggested by the proposed combination of references.

The Examiner takes the Official Notice that a device specific content packet is common and well known in the prior art in reference to network protocols. The Examiner further notes that this feature is commonly used by any system utilizing a network with digitally signed packets, commonly used in secure networks and content distribution systems. A device could utilize public key or digital certificate to “sign” data packets. When received these packets would only be able to be authenticated by a device with the proper corresponding key etc. (i.e. device specific content packet). This position is respectfully traversed relative to what is actually recited in Applicant’s claims.

By analyzing the Examiner’s reasoning in the light of the pending independent claims (e.g. claim 35) and assuming that the signed data packets correspond with the device specific content packets (which the Applicant does not agree with), it would mean that the header of the packet should contain information related to the description of the signed packet and information needed by the wireless device to run the signed packet. The content packet would also have to include a device specific content component with a data structure that includes information related to description properties of the device specific content component and information related to system attributes of the content component. Now, taking the header of Kaydyk to represent the data structure, the header would have to include all of the above mentioned information related to

description properties and system attributes. It would also have to include information needed to run the device specific content component. If the signed packet represented the device specific content component, the header would have to include information on how to check the signature and how to decrypt the signed packet. This would make the signature useless because anyone could obtain the header data and use it to verify the signature and decrypt the signed packet. The proposed combination of references does not support this.

Col. 136, lines 9—36 of Ginter discloses:

Many objects 300 that are distributed by physical media and/or by "out of channel" means (e.g., redistributed after receipt by a customer to another customer) might not include key blocks 810 in the same object 300 that is used to transport the content protected by the key blocks. This is because VDE objects may contain data that can be electronically copied outside the confines of a VDE node. If the content is encrypted, the copies will also be encrypted and the copier cannot gain access to the content unless she has the appropriate decryption key(s). For objects in which maintaining security is particularly important, the permission records 808 and key blocks 810 will frequently be distributed electronically, using secure communications techniques (discussed below) that are controlled by the VDE nodes of the sender and receiver. As a result, permission records 808 and key blocks 810 will frequently, in the preferred embodiment, be stored only on electronic appliances 600 of registered users (and may themselves be delivered to the user as part of a registration/initialization process). In this instance, permission records 808 and key blocks 810 for each property can be encrypted with a

private DES key that is stored only in the secure memory of an SPU 500, making the key blocks unusable on any other user's VDE node. Alternately, the key blocks 810 can be encrypted with the end user's public key, making those key blocks usable only to the SPU 500 that stores the corresponding private key (or other, acceptably secure, encryption/security techniques can be employed).

That kind of information relating to decryption of the packet cannot be delivered in the packet, but rather, it has to exist in the device which receives the signed packet. Therefore, Applicant respectfully submits that the cited references do not teach that *the content packet includes information needed by the wireless device to run the at least one device specific content component*, as is claimed by Applicant.

As to the rejection of claim 33, the Examiner appears to use the same arguments as in the rejection of claim 35. However, the subject matter of these claims are not equivalent. For example, claim 33 recites:

examining the data structure of the device specific content packet to identify download properties of the device specific content packet and compatibility of the at least one device specific content component with the particular wireless device;

selecting at least one device specific content component which said examining indicated is compatible with the particular wireless device;

Therefore, although the Examiner uses the authorization and signature of the content packet of Ginter, there is no disclosure about identifying download properties of the device specific content packet and selecting a content component compatible with the particular wireless device as claimed by Applicant. Therefore, Applicant respectfully submits that at least the rejection of claim 33, and claim 34 which refers to claim 33, are not valid.

Claim 35 is amended to recite a set of device specific content components for devices having different kind of properties, wherein a device specific content component can be selected from the set of content components according to the properties of the target device. This is not disclosed or suggested by the proposed combination of references. Page 12, lines 24—31 of the present application discloses:

Furthermore, the provider of the content packet can produce various versions of hardware-specific content components, for different communication device versions. The different content components of the content packet, the data structures of the content components, as well as said data structure of the content packet are transmitted to a content packet loading server 18a, 18b, in which they are preferably stored in a content packet database 19a, 19b.

This feature has originally been defined in the dependent claim 19 which is now combined with the independent system claim 43, which is also amended to recite a content packet server claim. Thus, claim 43 should now be allowable.

Dependent claim 45 recites that the content packet also comprises an installation application for installing the content packet in the wireless communication device. This is not disclosed or suggested by the proposed combination of references. This subject matter is disclosed on page 23, lines 1—3:

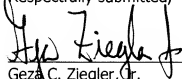
The content packet can also contain an installation application for installing the content packet in a wireless communication device.

This feature is not found in the combination of the cited references.

Therefore, it is respectfully submitted that claims 2-14, 16, 20, 24, 33-42 and 44-48 are not disclosed by the combination of Kaydyk, Ginter and Watanabe. Accordingly, allowance of the claims is solicited.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,



Geza C. Ziegler, Jr.
Reg. No. 44,004
Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

10 Feb 2009

Date